Deutscher Bundestag **Drucksache 18/10395**
18. Wahlperiode 11.11.2016

Unterrichtung

durch die Bundesregierung

Cyber-Sicherheitsstrategie für Deutschland 2016

Inhaltsverzeichnis

Zugeleitet mit Schreiben des Bundesministeriums des Innern vom 9. November 2016.

Einleitung

Die Digitalisierung in Staat, Wirtschaft und Gesellschaft hat Deutschland in nur wenigen Jahren grundlegend verändert. Neue Möglichkeiten der Kommunikation, des Wissenszugangs und der innovativen Gestaltung führen zu mehr sozialer Interaktion, neuen Geschäftsmodellen und neuen Feldern für Forschung und Entwicklung. Vernetzte elektronische Geräte prägen verstärkt den Lebens- und Arbeitsalltag der Menschen. Durch die zunehmende maschinelle Erzeugung von Daten sowie die zunehmende Verbreitung von intelligenten Zählern und Sensoren entstehen riesige Datenmengen. Selbstlernende Maschinen können immer komplexere Aufgaben übernehmen. Abläufe, Verfahren und Produktionsprozesse werden zunehmend vernetzt, Innovationszyklen immer kürzer. Der grenzüberschreitende Cyber-Raum erfordert neue Ansätze. Der Staat hat die Pflicht, diese Veränderungsprozesse im Interesse der Bürgerinnen und Bürger gemeinsam mit der Wirtschaft und weiteren Akteuren zu bewerten, aktiv zu gestalten und Rahmenbedingungen zu schaffen, um diese Veränderungsprozesse weiter zu entwickeln.

Die Digitalisierung eröffnet Chancen, birgt Risiken und braucht daher Vertrauen. Eine umfassende Sicherheit ist nicht erreichbar, ein Missbrauchspotential wird stets existieren. Aufgabe des Staates und der Wirtschaft ist es, die Grundlagen für dieses Vertrauen zu schaffen. Sicherheit ist hierbei ein wesentlicher Aspekt. Die Bürgerinnen und Bürger müssen auch zukünftig sicher, frei und selbstbestimmt agieren können. Dies gilt gerade dann, wenn sie die Technologien und die mit deren Einsatz verbundenen Risiken aufgrund steigender Komplexität nicht im Einzelnen nachvollziehen können. Unternehmen müssen ihr Know-how auch im Zeitalter der Digitalisierung vor einem unerlaubten Zugriff schützen und die Produktionsprozesse auch dann beherrschen, wenn dabei selbstlernende Maschinen zum Einsatz kommen oder ihre Daten durch die Nutzung von Cloud-Lösungen auf Servern in der ganzen Welt verteilt sind.

Mit der von der Bundesregierung im Februar 2011 beschlossenen „Cyber-Sicherheitsstrategie für Deutschland“ wurden wesentliche Weichenstellungen für eine zukunftsgerichtete Cyber-Sicherheitspolitik vorgenommen. Zahlreiche der darin vorgesehenen Maßnahmen sind seither umgesetzt worden. Als organisatorische Maßnahmen wurde mit dem Cyber-Sicherheitsrat an der Schaltstelle von Politik und Wirtschaft ein hochrangiges Gremium für strategische Impulse und mit dem Cyber-Abwehrzentrum eine Plattform für den strategischen und operativen Austausch zwischen den Behörden geschaffen. Cyber-Sicherheit ist inzwischen zu einem wesentlichen Baustein einer Vielzahl strategischer Konzepte und ressortübergreifender Vorhaben der Bundesregierung geworden. Es hat sich gezeigt, dass auch staatliche Institutionen zur Gewährleistung von Cyber-Sicherheit zunehmend vernetzt vorgehen müssen. Innere und äußere Sicherheit im Cyber-Raum sind nicht mehr trennscharf voneinander abzugrenzen. Die Wahrung der Cyber-Sicherheit und die Verteidigung gegen Cyber-Angriffe sind so zu einer gesamtstaatlichen Aufgabe geworden, die gemeinsam zu bewältigen ist.

Die strategischen Ansätze und Ziele der Cyber-Sicherheitsstrategie 2011 haben im Wesentlichen auch heute noch Bestand. Die sich stetig ändernden Rahmenbedingungen machen es aber erforderlich, sie zu ergänzen und in einer neuen ressortübergreifenden Strategie zu bündeln, die der Relevanz und Querschnittlichkeit des Themas Cyber-Sicherheit angemessen Rechnung trägt und dieses ganzheitlich erfasst.

Die Cyber-Sicherheitsstrategie 2016 bildet den ressortübergreifenden strategischen Rahmen für die Aktivitäten der Bundesregierung mit Bezügen zur Cyber-Sicherheit und schreibt die Cyber-Sicherheitsstrategie aus dem Jahr 2011 fort. Länder und Wirtschaft wurden in diesen Entwicklungsprozess mit einbezogen.

Cyber-Bedrohungslage

Die Cyber-Bedrohungslage in Deutschland ist von steigender Komplexität und Interdependenz der eingesetzten Technik und sich ständig wandelnden Bedrohungen geprägt. Mit der Digitalisierung moderner Gesellschaften wachsen zugleich deren Verwundbarkeit und das Missbrauchspotential im Cyber-Raum. Überdies wird die Privatsphäre der Bürgerinnen und Bürger zunehmend angreifbar.

Die Folgen von Cyber-Angriffen beschränken sich nicht auf den Cyber-Raum. Erfolgreiche Angriffe können gesellschaftliche, wirtschaftliche, politische und auch persönliche Schäden verursachen. Angriffe auf staatliche Institutionen mit dem Ziel der Ausspähung oder Sabotage können die Funktionsfähigkeit von Verwaltung, Streitkräften und Sicherheitsbehörden erheblich beeinträchtigen und damit Auswirkungen auf die öffentliche Sicherheit und Ordnung in Deutschland haben. Auch Cyber-Angriffe auf Energieversorgungsnetze können weite Bereiche des öffentlichen und privaten Lebens zum Erliegen bringen. Gezielte Cyber-Angriffe auf Bankeninfrastrukturen oder Börsenkursmanipulationen können zu einer Gefahr für die Finanzmärkte insgesamt werden und weitreichende Auswirkungen auf die Wirtschaft in Deutschland und der Welt haben. Die Manipulation beim automatisierten und vernetzten Fahren, der IT-gestützten Verkehrslenkung oder von IT-Anwendungen im Gesundheitswesen kann sehr reale und ernsthafte Gefahren für Leib und Leben der Bürgerinnen und Bürger herbeiführen. Die gezielte Verbreitung von Falschmeldungen, die durch gekaperte IT-Systeme ermöglicht wird, kann zur Desinformation und Manipulation der öffentlichen Meinung genutzt werden. Hierin bestehen langfristig Gefahren für die freiheitliche Gesellschaft und die Demokratie.

Die Angreifer haben vielfach einen kriminellen, extremistischen/terroristischen, militärischen oder nachrichtendienstlichen Hintergrund. Die quantitative und qualitative Vielfalt der potentiellen Akteure aus dem In- und Ausland und der technischen Möglichkeiten zur Verschleierung erschweren die Erkennung, Zuordnung, Abwehr und Verfolgung von Cyber-Angriffen. Politisch-militärische Konflikte werden oft von Cyber-Kampagnen begleitet oder unterhalb der Schwelle zum bewaffneten Konflikt auch im Cyber-Raum ausgetragen. Dies erschwert die politische Bewertung von Cyber-Angriffen und die Entscheidung über die gebotenen Gegenmaßnahmen.

Zahl und Qualität der Cyber-Angriffe nehmen dabei kontinuierlich zu und treffen auf oftmals unzureichend gesicherte IT-Systeme. Ein Teil der Angriffe weist einen hohen Professionalisierungsgrad auf. Angriffswerkzeuge sind mittlerweile sowohl für staatliche Akteure als auch für kriminelle Gruppen oder Individuen verfügbar. Insbesondere gegenüber technologisch hoch entwickelten Schadprogrammen reichen die klassischen Abwehrwerkzeuge häufig nicht mehr aus. Die Angreifer sind dabei technisch in der Lage, Cyber-Angriffe zu verbergen oder ihre Täterschaft zu verschleiern. Daher sind Cyber-Angriffe und deren Ursprung immer häufiger nicht, oder nur mit großem Aufwand und erheblicher Zeitverzögerung festzustellen. Es ist von einer Vielzahl bislang nicht erkannter Angriffe auszugehen. Staat, Wirtschaft und Gesellschaft in Deutschland werden von dieser Bedrohungslage in den kommenden Jahren in erheblichem Maße betroffen sein.

Leitlinien der Cyber-Sicherheitsstrategie

Die Handlungsfähigkeit und Souveränität Deutschlands müssen auch im Zeitalter der Digitalisierung gewährleistet sein. Eine zukunftsgerichtete Cyber-Sicherheitspolitik ermöglicht, dass unser Land die enormen Chancen und Potentiale der Digitalisierung im gesamtgesellschaftlichen Interesse voll ausschöpfen kann, indem die damit verbundenen Risiken beherrschbar werden.

Die Gewährleistung von Freiheit und Sicherheit zählt zu den Kernaufgaben des Staates. Dies gilt auch im Cyber-Raum. Aufgabe des Staates ist es daher, die Bürgerinnen und Bürger und Unternehmen in Deutschland gegen Bedrohungen aus dem Cyber-Raum zu schützen sowie Straftaten im Cyber-Raum zu verhindern und zu verfolgen. Ein Staat kann im Zeitalter der Digitalisierung nur dann dauerhaft seiner Aufgabe gerecht werden, wenn er für Wirtschaft und Gesellschaft auch im Cyber-Raum Schutz und Freiheit zur Entwicklung bietet und hierfür seine eigenen Systeme ausreichend sichert. Angesichts des digitalen Innovationspotenzials kommt es hierbei für den Staat darauf an, auf Basis einer entsprechenden Risikoanalyse mögliche Entwicklungen und deren Bedeutung für Fragen der Cyber-Sicherheit frühzeitig zu erkennen sowie neue Lösungsansätze zu erforschen und in politische Konzepte einzubinden.

Cyber-Sicherheit entsteht zuvorderst durch risikoangepasstes Verhalten und den Einsatz sicherer Systeme im Verantwortungsbereich des jeweiligen Betreibers und Anwenders. Bereits durch bewährte Basismaßnahmen, unter anderem die konsequente Anwendung risikoangemessener, wirksamer und aktueller Sicherheitsprodukte und Standards, kann eine Vielzahl von Cyber-Angriffen mit vertretbarem Aufwand abgewehrt werden.

Für die Prävention sowie das Erkennen, Zuordnen, Abwehren und Verfolgen von Cyber-Angriffen ist eine enge Zusammenarbeit und Koordinierung erforderlich. Staat, Wirtschaft, Wissenschaft und Gesellschaft tragen für die Sicherheit des Cyber-Raums eine gemeinsame Verantwortung. Sie müssen daher auch aufeinander abgestimmte Antworten auf die jeweils aktuellen Herausforderungen geben. Eine enge europäische und internationale Abstimmung ist dabei insbesondere auf Grund oftmals grenzüberschreitender Interdependenzen und Bedrohungen unter außen- und sicherheitspolitischen Gesichtspunkten unverzichtbar.

Als Konsequenz wird die Bundesregierung die Schwerpunkte ihrer Cyber-Sicherheitspolitik in den kommenden Jahren in folgenden vier Handlungsfeldern setzen:

1. Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung
2. Gemeinsamer Auftrag Cyber-Sicherheit von Staat und Wirtschaft
3. Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur
4. Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik

Die Maßnahmen in den jeweiligen Handlungsfeldern haben Querschnittscharakter und betreffen – in unterschiedlicher Ausprägung – alle gesellschaftlichen Bereiche.

Handlungsfeld 1: Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung

In einer digitalisierten Umgebung sicher und selbstbestimmt handeln zu können, ist ein wesentlicher Eckpfeiler von Cyber-Sicherheit. Die Bürgerinnen und Bürger müssen – ebenso wie Unternehmen, Staat und sonstige Akteure in Deutschland – in der Lage sein, die Chancen und Risiken beim Einsatz von Informationstechnik zu erfassen, zu bewerten und ihr Handeln daran auszurichten (Beurteilungskompetenz). Hierfür müssen die entsprechenden vertrauenswürdigen Technologien und Rahmenbedingungen vorliegen.

Die Möglichkeit zu einem sicheren und selbstbestimmten Handeln im Cyber-Raum steht im Kontext technologischer oder digitaler Autonomie. Grundlage hierfür ist eine gezielte digitale Bildung für alle Alters- und Anwendergruppen. Cyber-Sicherheit muss fest im Bewusstsein der Gesellschaft verankert werden, um digitaler Sorglosigkeit entgegenzuwirken.

Um die Chancen der Digitalisierung zu nutzen, muss für alle Anwendergruppen die Möglichkeit bestehen, auf vertrauenswürdige und sichere IT-Systeme zugreifen zu können und so die digitalen Verwundbarkeiten zu minimieren. Nutzerfreundliche und handhabbare Lösungen – gerade auch „Made in Germany" – auf Basis global nutzbarer technischer Architektur sind hier ein wichtiger Baustein, ebenso wie eine zielgerichtete IT-Sicherheitsforschung und -entwicklung, eine bedarfs- und anwendergerechte Zertifizierungspolitik sowie die Förderung von sicheren elektronischen Identitäten und der Verschlüsselung sowohl von elektronischer Kommunikation als auch von über das Internet angebotenen Diensten. Nationale Regelungen sind bei Bedarf den jeweils aktuellen Sicherheitserfordernissen anzupassen. Gleichzeitig wird sich die Bundesregierung in der Europäischen Union und in internationalen Organisationen auch weiterhin für angemessene und einheitliche IT-Sicherheitsstandards und wirksame gesetzliche Regelungen einsetzen.

Strategische Ziele und Maßnahmen

Digitale Kompetenz bei allen Anwendern fördern

Verantwortungsvolles Verhalten im Cyber-Raum und das Bewusstsein für die Chancen und spezifischen Risiken beim Einsatz von IT-Systemen sind integraler Bestandteil digitaler Kompetenz. Digitale Bildung muss daher künftig zu einem festen Bestandteil des Bildungskanons werden, von der Schule über die duale Ausbildung, die Hochschule bis hin zur beruflichen Weiterbildung und allgemeinen Erwachsenenbildung. Dies ist im schulischen und universitären Bereich vorrangig Aufgabe der Länder. Jede Schulabgängerin und jeder Schulabgänger sollte ein technisches Grundverständnis und grundlegende Kenntnisse im sicheren Umgang mit Informations- und Kommunikationstechnik haben. Bund und Länder müssen hier noch enger als bisher zusammenarbeiten. Die Bundesregierung wird insbesondere die duale Berufsausbildung konsequent auf die Erfordernisse einer digitalen Gesellschaft ausrichten und die Ausbildungsordnungen entsprechend anpassen. Überbetriebliche Bildungsstätten werden für das Zeitalter der Digitalisierung gerüstet. Diese müssen in der Lage sein, Weiterbildungen zur Digitalisierung auf hohem Niveau anzubieten. Die dafür erforderlichen Ausstattungsinvestitionen werden prioritär gefördert. Darüber hinaus wird sich die Bundesregierung bei Gewerkschaften und Arbeitgebern dafür einsetzen, Wege für eine flexiblere und individuellere digitale Weiterbildung zu schaffen.

Die Bundesregierung wird sich zudem für die Ausweitung des Lehrangebots durch Einrichtung von zusätzlichen Lehrstühlen und die Stärkung der vorhandenen Spitzeninstitute in den MINT-Bereichen und insbesondere in der Informatik einsetzen, etwa bei Big-Data-Analyse, industrieller Software und IT-Sicherheit. Dabei unterstützt die Bundesregierung auch eine stärkere Kooperation mit der Wirtschaft, etwa über drittmittelfinanzierte Stellen und Stiftungslösungen.

Digitaler Sorglosigkeit entgegenwirken

Neben Bildung bedarf verantwortungsvolles und risikobewusstes Handeln regelmäßiger Sensibilisierung, um digitaler Sorglosigkeit der Bürgerinnen und Bürger im privaten und beruflichen Umfeld entgegenzutreten. Die Bundesregierung wird daher in Zusammenarbeit mit Initiativen wie „Deutschland sicher im Netz e.V." die zielgruppengerechte Sensibilisierung vorantreiben. Sie fördert darüber hinaus gezielt Projekte, um die Medienkompetenz der Bürgerinnen und Bürger zu stärken. Die Initiativen der Bundesregierung aus dem Themenbereich „Cyber-Sicherheit und Gesellschaft" werden ausgebaut und weiterentwickelt. Dies schließt den gesellschaftlichen Diskurs zu übergreifenden politischen Fragestellungen im Themenkomplex Cyber mit gezielten Formaten ein. Auch in Unternehmen muss digitaler Sorglosigkeit entgegengetreten werden. Die Bestellung von IT-Sicherheitsbeauftragten, die – analog zum Datenschutzbeauftragten – Konzeption und Umsetzung von IT-

Sicherheitsmaßnahmen vorantreiben, ist hierzu ein probates und wirksames Mittel. Um Cyber-Bedrohungen sichtbarer zu machen, ist es zudem erforderlich, über aktuelle Erkenntnisse zu Sicherheitseigenschaften von IT-Produkten und Dienstleistungen zu informieren. Die Bereiche der öffentlichen Warnungen und Handlungsanleitungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) vor IT-Sicherheitslücken werden daher ausgebaut.

Voraussetzungen für sichere elektronische Kommunikation und sichere Webangebote schaffen

Eine sichere, vertrauliche, nicht manipulierbare elektronische Kommunikation ist grundlegend für die Wahrnehmung der Kommunikationsrechte, des Rechts auf Privatsphäre und der Persönlichkeitsrechte der Bürgerinnen und Bürger. Für Unternehmen ist sie ein wichtiger Schutz vor Cyber-Spionage und damit Grundlage für ihren wirtschaftlichen Erfolg. Eine leicht handhabbare und sichere Verschlüsselung gewährleistet eine vertrauliche elektronische Kommunikation für alle Akteure und sollte zum Standard werden. Forschungsvorhaben und Brancheninitiativen, die diesem Ziel dienen, werden von der Bundesregierung ausdrücklich begrüßt. Durch den konsequenten Einsatz starker Verschlüsselung bei Webangeboten wird die Sicherheit im Netz zusätzlich erhöht. Die Bundesregierung wird die spezifischen Hemmnisse beim Einsatz von Verschlüsselungslösungen untersuchen und Initiativen zum Abbau dieser Hemmnisse fördern.

Neben diesem Ansatz der „Sicherheit durch Verschlüsselung“ verfolgt die deutsche Krypto-Strategie gleichermaßen den Ansatz der „Sicherheit trotz Verschlüsselung“. Anwender müssen ihre Daten, Werte und Rechte auf höchstem Niveau schützen können. Gleichzeitig sind die deutschen Strafverfolgungs- und Sicherheitsbehörden unter strengen gesetzlichen Voraussetzungen befugt, verschlüsselte Kommunikation zu entschlüsseln oder zu umgehen, wenn dies im Einzelfall zur Erfüllung ihres gesetzlichen Auftrages notwendig ist. Um eine Aushöhlung dieser bereits bestehenden Befugnisse zu vermeiden, müssen die technischen Fähigkeiten der Strafverfolgungs- und Sicherheitsbehörden zur Entschlüsselung parallel zu den technischen Entwicklungen in Sachen Verschlüsselungen stetig fortentwickelt werden.

Sichere elektronische Identitäten

Parallel zu der Förderung einer sicheren elektronischen Kommunikation sind die Konzepte für eine sichere Identifikation von Personen und Dingen zu erweitern. Die Anwender müssen in die Lage versetzt werden, im Internet sichere, benutzerfreundliche und moderne Authentifizierungsmittel nutzen zu können. Das derzeit verbreitete, aber nicht sichere Benutzername/Passwort-Verfahren ist als Standard zu ergänzen und nach Möglichkeit abzulösen. Einen Kernpunkt stellen die Ausweisdokumente mit Online-Ausweisfunktion dar, mit dem die Bundesregierung bereits eine hochsichere und datensparsame Identifikationsmöglichkeit im Netz bereitstellt. Ziel ist es, die Online-Ausweisfunktion – und davon abgeleitete sichere Identitäten – als Standard-Identifizierungsmittel für sensible Dienste zu etablieren, fortzuentwickeln und vergleichbar sichere Lösungen auch in der Wirtschaft zu fördern.

Darüber hinaus setzt sich die Bundesregierung für ein einheitliches Identitätsmanagement in der gesamten deutschen Verwaltung ein und fordert die Anbieter von Informations- und Kommunikationstechnologie auf, gemeinsam mit der nationalen IT-Sicherheitsindustrie vertrauenswürdige Produkte und Dienstleistungen zu entwickeln und diese am Markt zur Verfügung zu stellen.

Zertifizierung und Zulassung stärken – Einführung eines Gütesiegels für IT-Sicherheit

Wirksame und bedarfsgerechte Zertifikate und Gütesiegel sind ein wichtiges Instrument für die Verbreitung von Cyber-Sicherheitsstandards. Die Zertifizierung oder Zulassung von IT-Sicherheitsprodukten ist bereits ein etabliertes und anerkanntes Verfahren. Zugleich deckt sie aber nur ein kleines Spektrum der Informationstechnik ab, die bei den Anwendern heute zum Einsatz kommt. Die Bundesregierung wirbt daher insbesondere bei Herstellern von Standardtechnologien für eine erhöhte Testierbereitschaft und wird ein Basis-Zertifizierungsverfahren für sichere IT-Verbraucherprodukte einführen, dessen Kriterien durch das BSI festgelegt werden. Parallel dazu werden die bestehenden Ressourcen im BSI zur Erarbeitung von technischen Richtlinien, zur Zertifizierung und zur Unterstützung der nationalen Akkreditierungsstelle im Bereich der IT-Sicherheit weiter gestärkt und die entsprechenden Prozesse im Interesse aller Beteiligten effizienter gestaltet. Dabei gilt es, der Herausforderung hochqualifizierter, aber zeitintensiver Zertifizierung und Zulassung bei kurzen Technologiezyklen durch moderne Prozesse zu begegnen. So kann etwa durch eine verstärkte Involvierung und Akkreditierung von Unternehmen sowie deren vertiefte Integration in den Zertifizierungsprozess diesen Herausforderungen effizient begegnet werden. Hierbei werden auch skalierbare und delegierte Prozesse gemäß BSI-Stan-

dards in Betracht gezogen. Die Bundesregierung wird sich für eine Ausweitung der europäischen und internationalen Anerkennungsabkommen für die IT-Sicherheitszertifizierung basierend auf gemeinsamen Sicherheitskriterien zur Bewertung von Sicherheitseigenschaften von Verfahren (Common Criteria und ISO/IEC 15408 sowie ISO/IEC 27000) einsetzen, um eine zunehmende internationale Anerkennung dieser Kriterien zu ermöglichen.

Die Kennzeichnung von IT-Sicherheitseigenschaften von Produkten und Dienstleistungen stellt in einigen Bereichen noch eine besondere Herausforderung dar. Um die Sicherheit von IT-Produkten und Dienstleistungen insbesondere für die Bürgerinnen und Bürger sowie kleine und mittelständische Unternehmen transparenter darzustellen, wird die Bundesregierung ihre Aktivitäten auf dem Gebiet der Gütesiegel und Zertifikate für IT-Sicherheit ausbauen und geeignete Vorschläge unterbreiten, insbesondere hinsichtlich übergreifender Systeme für die Zertifizierung und einer einheitlichen Kennzeichnung. Die Anwender sollen künftig auf Basis eines einheitlichen Gütesiegels bei der Kaufentscheidung für neue IT-Produkte und bei der Inanspruchnahme entsprechender Dienstleistungen leicht und schnell feststellen können, welches Angebot sicher ausgestaltet ist und hierdurch zum Schutz der Daten beiträgt. Cyber-Sicherheit soll dadurch für jedermann verständlicher und leichter realisierbar gemacht werden.

Digitalisierung sicher gestalten

Die Bürgerinnen und Bürger sowie die Unternehmen erwarten, dass die durch die Digitalisierung erfolgenden Veränderungen vom Staat bewertet und aktiv gestaltet werden. Beispiele hierfür sind das E-Health-Gesetz sowie das IT-Sicherheitsgesetz. Dieser Weg muss konsequent weiter beschritten werden. Hierbei werden neue Technologien, neue Geschäftsmodelle und ein sich wandelndes Anwenderverhalten ebenso zu berücksichtigen sein wie neue Bedrohungen sowie neue europäische und internationale Vorgaben, zum Beispiel durch die EU-Richtlinie zur Netz- und Informationssicherheit. Vorgaben für eine angemessene Verteilung von Verantwortlichkeiten und Sicherheitsrisiken im Netz zum Beispiel durch Produkthaftungsregeln für IT-Sicherheitsmängel und Sicherheitsvorgaben für Hard- und Softwarehersteller werden geprüft. Bereits bei der Erstellung von Gesetzen und Verordnungen des Bundes sollten zudem die Auswirkungen des Einsatzes digitaler Technologien, insbesondere auf die Cyber-Sicherheit, berücksichtigt werden.

Daneben soll die frühzeitige Umsetzung von Sicherheitsanforderungen rechtlich eingefordert werden können, um deren Berücksichtigung bereits am Beginn einer technischen Entwicklung (Security-by-design) sicherzustellen. Zu diesem Zweck steht das BSI den Bundesressorts als zentrale Beratungsstelle zur Verfügung.

Die Digitalisierung der Mobilität und der damit verbundene Zuwachs an Daten stellen neue grenzüberschreitende Anforderungen an die Sicherheit von Fahrzeugen und Infrastruktur sowie an den Schutz der Persönlichkeitsrechte. Deutschland wird sich aktiv für die Schaffung internationaler Standards insbesondere auf Ebene der UNECE einsetzen, um für ausreichenden Schutz vor Manipulationen und Missbrauch der technischen Strukturen als auch der Daten und Prozesse zu sorgen.

IT-Sicherheitsforschung vorantreiben

Um die Chancen der Digitalisierung in allen Bereichen wie zum Beispiel Industrie 4.0, Medizintechnik und Mobilität 4.0 voll auszuschöpfen, werden neue, ganzheitliche IT-Sicherheitslösungen benötigt. Daher müssen bereits heute innovative IT-Sicherheitslösungen von morgen erforscht und umgesetzt werden. Die Bundesregierung baut hierfür das Forschungsrahmenprogramm zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt 2015 - 2020“ weiter aus und vernetzt dieses eng mit den anderen Maßnahmen der Cyber-Sicherheitsstrategie.

In diesem Zusammenhang werden auch die bestehenden Kompetenzzentren für IT-Sicherheitsforschung CRISP (Darmstadt), CISPA (Saarbrücken) und KASTEL (Karlsruhe) weiter gestärkt. Diese greifen kontinuierlich aktuelle Forschungsthemen auf, stellen Einschätzungen und Bewertungen für die Politik bereit und entwickeln konkrete Lösungen. Die in zahlreichen staatlich geförderten Projekten entwickelten anwendungsbezogenen Forschungsergebnisse sollen möglichst schnell in Produkte und Verfahren umgesetzt und vermarktet werden. Für den militärischen Anwendungsbereich der IT- und Cyber-Sicherheit übernimmt diese Aufgabe der Cyber-Cluster an der Universität der Bundeswehr in München mit dem Forschungsinstitut Cyber Defence und Smart Data (CODE). Die kommerzielle Nutzung und Weiterentwicklung innovativer und neuer Ideen in der IT-Sicherheit in Unternehmen und Startups soll explizites Ziel und Bestreben staatlicher Investitionen sein, um so einen möglichst hohen volkswirtschaftlichen Nutzen zu realisieren. Parallel kann das aktive Technologie-Scouting dazu beitragen, dass modernste Technologien schnell entdeckt, eingeführt und weiterentwickelt werden. Auch private Venture Capital-Investoren können an dieser Stelle eine wichtige Rolle spielen.

Handlungsfeld 2: Gemeinsamer Auftrag von Staat und Wirtschaft

Eine vertrauensvolle Zusammenarbeit und ein enger Austausch zwischen Staat und Wirtschaft sind unabdingbar, um Cyber-Sicherheit in Deutschland dauerhaft auf einem hohen Niveau gewährleisten zu können. Dabei sind im Sinne eines kooperativen Ansatzes auch neue Wege zu beschreiten, um die jeweiligen Kompetenzen zu bündeln und zu nutzen.

Die Unternehmen in Deutschland müssen in der Lage sein, sich selbst und ihre Kunden wirksam vor Cyber-Angriffen zu schützen. Besonderes Augenmerk gilt dabei den Betreibern Kritischer Infrastrukturen. Aber auch andere Unternehmen können für Staat, Wirtschaft und Gesellschaft von hoher Relevanz sein und müssen besonders geschützt werden. Hierfür sind im Wege des mit dem IT-Sicherheitsgesetz etablierten kooperativen Ansatzes die erforderlichen Rahmenbedingungen fortzuentwickeln und bei Bedarf auf andere Bereiche der Wirtschaft zu erweitern. Bei der Entwicklung und Durchsetzung wirksamer und bedarfsgerechter IT-Sicherheitsstandards müssen Staat und Wirtschaft vertrauensvoll und eng zusammenarbeiten. Das Fundament hierfür ist eine starke deutsche IT-Wirtschaft, die durch eine moderne Wirtschaftspolitik zu fördern ist. Die Bundesregierung wird zudem Maßnahmen erarbeiten, um die im internationalen Vergleich schwächer ausgeprägte Gründungskultur für Startups im Bereich IT-/Cyber-Sicherheit in Deutschland zu verbessern. Der Einbeziehung von Providern und nationalen IT-Sicherheitsdienstleistern kommt bei der Erkennung und Abwehr von Cyber-Angriffen eine Schlüsselrolle zu.

Strategische Ziele und Maßnahmen

Kritische Infrastrukturen sichern

Der Schutz Kritischer Infrastrukturen steht im Zentrum der gemeinsamen Aktivitäten von Staat und Wirtschaft. Angesichts der Vernetzung der Systeme kommt dabei dem Schutz der IT Kritischer Infrastrukturen besondere Bedeutung zu. Dies ist eine ressortgemeinsame und gesamtstaatliche Aufgabe der Cyber-Abwehr und -Verteidigung, da innere und äußere Sicherheit im Bereich Cyber eng zusammenfallen. Bei der Umsetzung der mit dem IT-Sicherheitsgesetz getroffenen Vorgaben müssen Staat und Wirtschaft (unter anderem im Rahmen der öffentlich-privaten Partnerschaft des UP KRITIS) auf allen Ebenen eng zusammenarbeiten und einen vertrauensvollen Informationsaustausch etablieren. Mindeststandards und Meldewege werden gemeinsam mit der Wirtschaft erarbeitet, umgesetzt und fortentwickelt. Zudem wird die Ausweitung solcher Präventions- und Reaktionspflichten auch auf andere Unternehmen von hoher gesellschaftlicher Relevanz geprüft.

Unternehmen in Deutschland schützen

Die Bundesregierung wird ihre Sensibilisierungs- und Unterstützungsangebote für die deutsche Wirtschaft ausbauen und stärker vernetzen. Gerade mittelständische Unternehmen müssen in die Lage versetzt werden, sich wirksam vor den Gefahren im und aus dem Cyber-Raum zu schützen, um die mit der Digitalisierung verbundenen Chancen in vollem Umfang nutzen zu können. Umsetzungsstrategien dazu sind gemeinsam durch Staat, Wissenschaft und Wirtschaft zu entwickeln. Unternehmen sollen durch den Staat konkret dabei unterstützt werden, das für sie notwendige IT-Sicherheitsniveau zu erreichen. Das Vertrauen zwischen Unternehmen und Behörden in Diskretion und Professionalität im Umgang mit sensiblen Sachverhalten spielt hierbei eine wesentliche Rolle.

Zur Abwehr von Cyber-Kriminalität und Cyber-Spionage gegen Unternehmen leisten insbesondere die „Zentrale Ansprechstelle Cyber-Crime der Polizeien der Länder und des Bundes“ sowie das Bundesamt für Verfassungsschutz (BfV) wesentliche Beiträge. Die Bundesregierung wird zudem Angebote wie die Allianz für Cyber-Sicherheit, das „German Competence Center against Cyber-Crime (G4C)“, die Initiative „IT-Sicherheit in der Wirtschaft“ sowie die „Initiative Wirtschaftsschutz“ gemeinsam mit Partnern aus Wirtschaft und Wissenschaft ausbauen und – auch zur Schaffung von Synergieeffekten – stärker vernetzen.

Die deutsche IT-Wirtschaft stärken

Cyber-Sicherheit in Deutschland erfordert eine starke und innovative deutsche IT-Wirtschaft. Grundlage sind die Identifikation von Schlüsseltechnologien im IT-Sicherheits- und Verteidigungsbereich aus der Hand von vertrauenswürdigen IT-Herstellern sowie sichere Netzinfrastrukturen. Um die Wettbewerbsfähigkeit der nationalen IT-Sicherheitswirtschaft zu stärken, wird die Bundesregierung das Qualitätsmerkmal „IT-Security Made in Germany“ fördern und Außenwirtschaftsinstrumente ausbauen. In nationalen Schlüsseltechnologiefeldern

sind die Vernetzung mit der nationalen IT-Sicherheitswirtschaft zu stärken und – wo möglich und sinnvoll – eigene Kapazitäten aufzubauen, zu fördern und zu schützen.

Es bedarf darüber hinaus eines breiteren Portfolios qualifizierter, vertrauenswürdiger Dienstleister, zum Beispiel für IT-Sicherheitslösungen, Forensik, Angriffserkennung und -reaktion. Auch hier sollen die Anwender zukünftig auf einen breiteren Markt von Dienstleistern zurückgreifen können. IT-Unternehmen werden durch die Bundesregierung im Kontext spezieller Forschungsprogramme gefördert. Sie entwickeln in gemeinsamen Projekten mit Hochschulen, außeruniversitären Forschungseinrichtungen und anderen Partnern aus der Wirtschaft innovative Ansätze für neue Produkte und Dienstleistungen.

Mit den Providern zusammenarbeiten

Eine Schlüsselrolle kommt der Zusammenarbeit mit den Providern zu. Dies gilt im Rahmen des geltenden Rechts insbesondere für Maßnahmen der Provider zur Erkennung von Cyber-Bedrohungen, zum Umgang mit erkannten Vorfällen/Infektionen und zur Abschwächung laufender Angriffe. Der Ausbau datenschutzkonformer Sensorik zur Anomalieerkennung im Netz ist hierbei ein wirksames Mittel, um die Datensicherheit im Netz generell zu erhöhen. Um die Rechte der Betroffenen zu schützen, sollen die Erkenntnisse anonymisiert bzw. pseudonymisiert werden.

IT-Sicherheitsdienstleister einbeziehen

In Zeiten des IT-Fachkräftemangels haben Staat und Wirtschaft ein Interesse daran, den gegenseitigen Austausch von IT-Fachwissen und die Bildung von Spezialisten-Netzwerken zu befördern. Im Rahmen des geltenden Rechts werden zukünftig private IT-Sicherheitsdienstleister im Bedarfsfall stärker als in anderen Bereichen staatlichen Handelns eingebunden. Die Bundesregierung wird daher gezielt Möglichkeiten zur Förderung kompetenter und vertrauenswürdiger IT-Sicherheitsdienstleister wahrnehmen. Sie wird darüber hinaus gemeinsam mit Vertretern der deutschen IT-Sicherheitswirtschaft personelle Austauschprogramme im Cyber-Sicherheitsbereich konzipieren und umsetzen. Der staatlichen Geheimhaltung und dem Schutz von Dienstgeheimnissen ist dabei ebenso Rechnung zu tragen wie dem Schutz von Betriebs- und Geschäftsgeheimnissen der Unternehmen.

Eine Plattform für vertrauensvollen Informationsaustausch schaffen

Der kooperative Ansatz umfasst auch den intensiven gegenseitigen Informationsaustausch. Die Bundesregierung wird hierfür eine Kooperationsplattform für Staat und Wirtschaft institutionalisieren, die innerhalb der vorgegebenen rechtlichen Grenzen vor allem einen Austausch relevanter Lageinformationen zur Abwehr von Cyber-Angriffen ermöglicht.

Handlungsfeld 3: Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur

Der Staat muss Sicherheit, Recht und Freiheit in unserem Land auch im Cyber-Raum gewährleisten. Hierzu bedarf es einer zeitgemäßen Cyber-Sicherheitsarchitektur, die die verschiedenen Akteure auf Bundesebene wirksam verzahnt und daneben die Länder, Kommunen und die Wirtschaft im Blick behält.

Die fortschreitende Digitalisierung führt dazu, dass heute eine Vielzahl von staatlichen Stellen in Bund und Ländern mit Fragen der Cyber-Sicherheit befasst ist. Das Aufgabenfeld ist breit und reicht – unter Beachtung der verfassungsrechtlich gebotenen Grenzen – von der Prävention, der Gefahrenabwehr und der Strafverfolgung über die Spionageabwehr und nachrichtendienstliche Aufklärung bis zur Cyber-Verteidigung. Dabei sind sowohl innere wie äußere Sicherheit im Cyber-Raum gleichermaßen betroffen. Der Staat muss seine Institutionen so aufstellen, dass sie ihren Schutzauftrag für die Gesellschaft auch im Zeitalter der Digitalisierung wahrnehmen können, und sich selbst wirksam gegen Cyber-Angriffe sichern.

Eine moderne Cyber-Sicherheitsarchitektur begreift Cyber-Sicherheit vor diesem Hintergrund als permanente gesamtstaatliche Aufgabe, die gemeinsam zu bewältigen ist. Wesentlich ist, dass im Bedarfsfall Informationen verteilt werden und die Aufgabenwahrnehmung effizient koordiniert wird. Föderalen, ressort- und behördensowie grenzübergreifenden Synergien kommt besondere Bedeutung zu. Das Nationale Cyber-Abwehrzentrum bietet auf Bundesebene bereits die entsprechende Struktur, unter deren Dach die einzelnen Akteure im Rahmen ihrer jeweiligen Zuständigkeiten zusammenarbeiten. Es gilt, diese Zusammenarbeit zu intensivieren und die Länder künftig stärker einzubinden. Die Bundesregierung wird dabei die rechtlichen Zuständigkeiten sowie die technischen und personellen Fähigkeiten überprüfen, eng aufeinander ausrichten und – wo erforderlich – anpassen. Nur so kann die staatliche Handlungsfähigkeit zur Prävention, Erkennung, Aufklärung, Abwehr und Verfolgung von Cyber-Angriffen auch im Zeitalter der Digitalisierung erhalten bleiben.

Strategische Ziele und Maßnahmen

Das Nationale Cyber-Abwehrzentrum weiterentwickeln

Im Rahmen der Umsetzung der Cyber-Sicherheitsstrategie 2011 wurde mit Gründung des Nationalen Cyber-Abwehrzentrums (Cyber-AZ) unter Federführung des Bundesministeriums des Innern der Informationsaustausch zwischen den relevanten Bundesbehörden gestärkt. Derzeit tauschen die für Cybersicherheitsfragen zuständigen Bundesbehörden im Cyber-AZ Informationen zu Cyber-Vorfällen aus und teilen ihre Bewertungen und Analysen.

Dieser Weg soll weiter beschritten und intensiviert werden. Zur Stärkung der Cyber-Abwehrfähigkeit muss im Rahmen der gesamtstaatlichen, ressortübergreifenden Cyber-Sicherheitsarchitektur auch das Cyber-AZ in geeigneter Weise aufgestellt und organisatorisch gestärkt werden. Als ressortgemeinsame Institution wird es unter Federführung des Bundesministeriums des Innern zur zentralen Kooperations- und Koordinationsplattform fortentwickelt. Das Cyber-AZ soll zukünftig mit eigenen Bewertungs- und Auswertungsfähigkeiten ausgestattet sein und über ein aktuelles Cyber-Lagebild verfügen, das die Cyber-Sicherheitslage in Deutschland widerspiegelt. Bei Cyber-Angriffen ist eine gegenseitige Unterrichtung und Abstimmung aller nationalen Akteure im Rahmen des geltenden Rechts von großer Bedeutung. Haben Cyber-Angriffe ihren Ursprung im Ausland, müssen außen- und sicherheitspolitische Aspekte miteinbezogen werden. Bei Cyber-Sicherheitsvorfällen, die bundesweit zahlreiche Institutionen betreffen, wächst das Cyber-AZ zu einem Krisenreaktionszentrum auf; in diesen Fällen können die Sicherung und Wiederherstellung der IT-Systeme sowie die Aufklärung und Abwehr von Cyber-Angriffen nur durch abgestimmte Maßnahmen der nationalen Akteure erreicht werden. Diese operative Zusammenarbeit soll intensiver koordiniert werden. Auch die Konzeption und Durchführung von gemeinsamen Übungen und gegenseitiger Fortbildung sind zu etablieren.

Die Länder sind eingeladen, in diesen Abstimmungsprozess ihre Fähigkeiten im Rahmen der gesamtstaatlichen Aufgabenwahrnehmung einzubringen.

Die Fähigkeit zur Analyse und Reaktion vor Ort stärken

Cyber-Angriffe der letzten Zeit haben gezeigt, dass es kaum institutionalisierte staatliche Strukturen gibt, die Betroffenen zeitnah vor Ort über die üblichen IT-Sicherheitsmaßnahmen hinaus bei der Aufbereitung eines Vorfalls helfen können. Hierbei geht es zum einen um die technische Bewältigung von Sicherheitsvorfällen, für die eine besondere Expertise im BSI vorhanden ist. Zum anderen können Cyber-Angriffe ein Tätigwerden der Sicherheitsbehörden vor Ort auf der jeweiligen gesetzlichen Grundlage erforderlich machen. Die notwendige

Koordination bei solchen Einsätzen verschiedener Behörden erfolgt unter Wahrung der rechtlichen Grenzen im Nationalen Cyber-Abwehrzentrum. Dabei werden die jeweiligen Wiederherstellungs-, Aufklärungs- und Strafverfolgungsinteressen der eingesetzten Behörden ebenso wie die Schutzinteressen der betroffenen Stelle beachtet.

Im BSI werden „Mobile Incident Response Teams“ (MIRTs) eingerichtet, die Cyber-Vorfälle in den für das Gemeinwesen besonders bedeutenden Einrichtungen analysieren und bereinigen sollen. Die MIRTs des BSI werden in der Lage sein, auf Ersuchen Verfassungsorgane, Bundesbehörden sowie Betreiber Kritischer Infrastrukturen und vergleichbar wichtiger Einrichtungen vor Ort schnell, flexibel und adressatengerecht bei der technischen Bewältigung von Sicherheitsvorfällen zu unterstützen, wenn hieran ein besonderes öffentliches Interesse besteht. Ziel dieser Unterstützung ist die schnelle Wiederherstellung eines sicheren technischen Betriebs der betroffenen Einrichtung.

Cyber-Angriffe können auch das Tätigwerden der Sicherheitsbehörden des Bundes vor Ort erforderlich machen. Im Bundeskriminalamt (BKA) erfolgt dafür die Einrichtung einer spezialisierten Ermittlungseinheit (Quick Reaction Force (QRF)), die in Absprache mit der zuständigen Staatsanwaltschaft oder Bundesanwaltschaft die ersten unaufschiebbaren strafprozessualen Maßnahmen für die Strafverfolgungsbehörden umsetzt. Im BfV werden „Mobile Cyber-Teams aufgebaut, bestehend aus IT-Spezialisten, nachrichtendienstlichen Fachleuten mit Erfahrung in der Auswertung von Cyber-Angriffen und – bei Bedarf – fremdsprachigen Mitarbeitern. Bei einem Cyber-Angriff mit nachrichtendienstlichem oder extremistischem/terroristischem Hintergrund kommen diese Cyber-Teams vor Ort zum Einsatz. Das betrifft auch mögliche Sabotageangriffe Im Verteidigungsbereich übernimmt diese Aufgabe der Militärische Abschirmdienst (MAD). Der Bundesnachrichtendienst (BND) kann – unter Beachtung seiner rechtlichen Möglichkeiten – einen Angriff sowohl in der Vorbereitungs- als auch in der Durchführungsphase beobachten. Zusätzlich werden aus den Angriffen resultierende Informationsabflüsse registriert. Auch die Bundeswehr kann mit ihren Organisationselementen (u.a. Incident Response Teams) – innerhalb der verfassungsrechtlichen Grenzen – Beiträge zur gesamtstaatlichen Sicherheitsvorsorge leisten.

Darüber hinaus sind schwerwiegende Cyber-Angriffe vorstellbar, gegen die mit den klassischen präventiven Maßnahmen in der notwendigen Zeit nicht nachhaltig vorgegangen werden kann. Die Bundesregierung wird daher prüfen, unter welchen rechtlichen Rahmenbedingungen und mit welchen technischen Möglichkeiten in diesen Fällen durch staatliche Stellen Netzwerkoperationen durchgeführt werden könnten.

Strafverfolgung im Cyber-Raum intensivieren

Die Bundesregierung wird ihre Anstrengungen zur Bekämpfung von Cyber-Kriminalität in den kommenden Jahren weiter intensivieren. Hierzu ist ein enger Informationsaustausch und Wissenstransfer auf nationaler und internationaler Ebene zu gewährleisten.

Besondere Bedeutung kommt zudem der weiteren technischen und fachlichen Befähigung von Justiz und Strafverfolgungsbehörden zu. Die entsprechenden bedarfsorientierten Aus- und Fortbildungsinhalte werden weiterentwickelt. Die Bundesregierung wird sich zudem dafür einsetzen, dass im Rahmen der Personalentwicklung die Voraussetzungen für die Gewinnung und Entwicklung von qualifiziertem Personal in den Aufgabenbereichen Aufklärung, Cyber-Kriminalität und digitale Forensik verbessert werden.

Bei den Sicherheitsbehörden des Bundes und der Länder sollten leistungsstarke Analyse- und Auswertesysteme aufgebaut werden.

Bei neuen Technologien wird sich die Bundesregierung dafür einsetzen, dass Befugnisse und Fähigkeiten der Sicherheitsbehörden mit den aktuellen Entwicklungen Schritt halten, damit keine Lücken in der Gefahrenabwehr und Strafverfolgung entstehen. Ermittlungsmaßnahmen im Bereich der informationstechnischen Überwachung müssen technikoffen ausgestaltet werden. So ist gewährleistet, dass ihre Umsetzung nach dem Stand der Technik möglich ist und effizient gestaltet werden kann.

Cyber-Spionage und Cyber-Sabotage effektiv bekämpfen

Für ausländische Nachrichtendienste stellen Cyber-Angriffe auf IT-Systeme von staatlichen Stellen, Wirtschaftsunternehmen und Forschungseinrichtungen sowie deren Beschäftigte eine bedeutende Methode der Informationsbeschaffung dar. Die Bundesregierung ist dem mit einer Neuausrichtung der Spionageabwehr entgegengetreten und wird den eingeschlagenen Weg des verstärkten 360-Grad-Blickes, also der Beobachtung grundsätzlich aller Aktivitäten fremder Nachrichtendienste in Deutschland, fortsetzen. Die Abteilung Spionageabwehr im BfV wird hierzu personell weiter verstärkt und organisatorisch zielgenauer strukturiert. Die Abwehr

von Cyber-Spionage (d.h. die technische und fachliche Analyse sowie Bewertung der gegen Bundesbehörden und sonstige Ziele gerichteten Angriffe mit mutmaßlich nachrichtendienstlichem Hintergrund) bildet hierbei einen Schwerpunkt. Darüber hinaus wird das BfV noch intensiver gegen Cyber-Angriffe mit extremistischem und terroristischem Hintergrund vorgehen.

Ein Frühwarnsystem gegen Cyber-Angriffe aus dem Ausland

Der BND erfasst gemäß seinem gesetzlichen Auftrag im Ausland Cyber-Spionage- und sonstige Cyber-Angriffe, die sich gegen staatliche und/oder Kritische Infrastrukturen in Deutschland richten. Diesen kann der BND frühzeitig Warnhinweise zur Einleitung von Abwehrmaßnahmen geben (Signals Intelligence Support to Cyber Defense (SSCD)). Der BND baut so mit IT-Spezialisten und erfahrenen Analysten ein Frühwarnsystem gegen Cyber-Angriffe auf. Die erkannten Angriffe werden qualitativ und quantitativ bewertet, um darüber ein aktuelles Lagebild der Bedrohungslage zu entwickeln.

Gründung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)

Die nationalen Sicherheitsbehörden müssen im digitalen Umfeld ebenso wirksam agieren können wie in anderen Bereichen. Zur Erzielung von Synergieeffekten wird für diese Zukunftsaufgabe im Geschäftsbereich des Bundesministeriums des Innern eine zentrale Stelle für die technische Unterstützung der Sicherheits- und Fachbehörden des Bundes einschließlich der Nachrichtendienste im Hinblick auf deren operativen Cyber-Fähigkeiten eingerichtet. Die Aufgaben orientieren sich am Aufgabenspektrum dieser Behörden und haben unterstützenden Charakter. Schwerpunktmäßig ergeben sich die drei Aufgabengebiete Entwicklung, Unterstützung und Beratung der Sicherheitsbehörden. Die zu gründende Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) erarbeitet hierfür in enger Zusammenarbeit mit den genannten Behörden bedarfsbezogen und zukunftsorientiert Methoden, Produkte und (übergreifende) Strategien zur operativen Umsetzung in den Sicherheitsbehörden und entwickelt diese bedarfsgerecht fort. ZITiS selbst erhält keine operativen Befugnisse.

Verteidigungsaspekte der Cyber-Sicherheit stärken

Cyber-Verteidigung ist als militärischer Teil der Gesamtverteidigung verfassungsmäßiger Auftrag der Bundeswehr und unterliegt den für Einsätze der Bundeswehr geltenden nationalen wie völkerrechtlichen Regelungen. Verteidigungsaspekte der gesamtstaatlichen Cyber-Sicherheit sind gemäß Weißbuch 2016 originäre Aufgaben des Bundesministeriums der Verteidigung und der Bundeswehr. Cyber-Abwehr, Cyber-Außen- und internationale Cyber-Sicherheitspolitik sowie Cyber-Verteidigung sind drei ergänzende Mittel zum Erreichen von Cyber-Sicherheit. Die Verteidigungsfähigkeiten der Bundeswehr im Cyber-Raum sind aber auch wesentlicher Teil der Cyber-Sicherheitsarchitektur. Sowohl die inhaltliche Übereinstimmung bei der technischen Umsetzung von Schutzmaßnahmen als auch die Nutzung und Mitgestaltung von Strukturen, Prozessen und Meldewesen der Cyber-Abwehr unter verteidigungsrelevanten Aspekten und Situationen zeigen die enge Abhängigkeit. Die Bundeswehr ist als hochtechnisierte Armee im weltweiten Einsatz den Gefahren im Cyber-Raum fortlaufend ausgesetzt. Gleichzeitig ist die Nutzung des Cyber-Raums Voraussetzung für die Einsatzfähigkeit der Streitkräfte.

Cyber-Verteidigung und Cyber-Abwehr sind in sämtliche Planungen, Strukturen und Prozesse der Gesamtverteidigung zu integrieren. Informationssicherheit und der Schutz des IT-Systems der Bundeswehr werden rund-um-die Uhr sowohl in den Einsatzgebieten als auch in Deutschland im Sinne einer Dauereinsatzaufgabe sichergestellt. Damit die Bundeswehr ihre Aufgaben im Cyber-Raum wahrnehmen kann, werden die bundeswehreigenen Fähigkeiten ausgebaut, die Sicherheitsarchitektur ihrer IT-Systeme konsolidiert sowie die bisher fragmentierten Strukturen in einer ministeriellen Abteilung und einem neuen eigenständigen militärischen Organisationsbereich zusammengeführt.

Die Bundeswehr verfügt darüber hinaus über besondere Expertise, Fähigkeiten und Ressourcen, die in Form der Amtshilfe – im Rahmen der verfassungsrechtlichen Grenzen – auch anderen staatlichen Akteuren nutzbar gemacht werden können. Sie kann durch Leistungen ziviler Unternehmen zur Erfüllung ihres verfassungsrechtlichen Auftrages unterstützt werden.

CERT-Strukturen in Deutschland stärken

Staatliche und nichtstaatliche „Computer Emergency Response Teams“, kurz „CERTs“, sind als zentrale Anlaufstellen für präventive und reaktive technische Maßnahmen im IT-Sicherheitsbereich ein wichtiger Baustein jeder nachhaltigen Cyber-Sicherheitsarchitektur. Durch sie wird weltweit der Notwendigkeit von Informationsaustausch und Koordination auf der informationstechnischen Fachebene Rechnung getragen. In Deutschland nimmt das BSI mit dem CERT-Bund für die Verwaltung sowie seinen Angeboten für Betreiber Kritischer Infrastrukturen, die Wirtschaft und Bürgerinnen und Bürger sowie als zentrale Ansprechstelle für ausländische und internationale CERTs die Rolle des nationalen CERTs wahr. Weitere eigenständige CERTs existieren zudem bei anderen Bundesbehörden sowie in den Länderverwaltungen, in einzelnen Unternehmen und in wissenschaftlichen Einrichtungen. Diese Strukturen müssen im Interesse gesamtgesellschaftlicher Cyber-Sicherheit weiter ausgebaut und vernetzt werden. Das BSI wird die Zusammenarbeit im Verwaltungs-CERT-Verbund (Bund-Länder) sowie mit Unternehmens- und Wissenschafts-CERTs weiter intensivieren und alle wesentlichen Akteure an einen Tisch bringen. Die bestehenden CERT-Strukturen in Deutschland sollen so unter Wahrung des Erreichten in einem gemeinsamen Prozess vervollständigt und verbessert werden. Dabei ist die Entwicklung des Cyber-AZ zu berücksichtigen.

Die Bundesverwaltung sichern

Die rasante technologische Entwicklung, die zunehmende Komplexität der Informations- und Kommunikationstechnik sowie die Digitalisierung der Verwaltung stellen auch in der Bundesverwaltung neue Anforderungen an das IT-Sicherheitsmanagement. Der „Umsetzungsplan für die Gewährleistung der IT-Sicherheit in der Bundesverwaltung“ (Umsetzungsplan Bund – UP Bund) als verbindliche IT-Sicherheitsleitlinie für alle Behörden des Bundes wird hierfür auf die aktuellen technischen wie organisatorischen Entwicklungen neu ausgerichtet.

Mit dem Gesamtprojekt „IT-Konsolidierung Bund“ wird die grundsätzliche Zusammenführung der IT-Betriebe der unmittelbaren Bundesverwaltung angestrebt. Ein Kernziel ist dabei auch die Stärkung der IT-Sicherheit. Mit dem Projekt „Netze des Bundes“ wird eine einheitliche und sichere Netzinfrastruktur der Bundesverwaltung geschaffen. In einem ersten Schritt werden hierfür die vom Bundesministerium des Innern verantworteten Bestandsnetze auf ein gemeinsames Netz migriert und so ein einheitliches, erhöhtes IT-Sicherheitsniveau etabliert. Um in Zukunft eine schrittweise Migration der übrigen Netze der Bundesverwaltung zu erreichen, wird das gemeinsame Netz auch als Integrationsplattform für alle IT-Netze der Bundesverwaltung fungieren.

Die Bundesregierung hat darüber hinaus ein Programm zur Förderung der sicheren mobilen Kommunikation aufgesetzt. Neben der Sensibilisierung für den Einsatz von sicheren IT-Produkten wird auch auf die Berücksichtigung von sicherheitsrelevanten Eigenschaften bei Beschaffungen hingewirkt werden. Zudem wird die Resilienz der IT-Systeme des Bundes erhöht, um Schadensfälle, die sich nicht vermeiden lassen, besser kompensieren zu können.

Zwischen Bund und Ländern eng zusammen arbeiten

Für die Bereiche Cyber-Kriminalität, Cyber-Spionage und präventive Eigensicherung der Verwaltungen bestehen im Bund-Länder-Verhältnis bewährte Gremienstrukturen. Um die Bund-Länder-Zusammenarbeit zusätzlich zu stärken, soll dem BSI die Unterstützung von Landesbehörden als neue Aufgabe übertragen werden, soweit diese mit der Bewältigung von Cyber-Sicherheitsvorfällen befasst sind. Bisher gilt dies nur für die Unterstützung von Polizeien und Strafverfolgungsbehörden.

Mit der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung“, die der IT-Planungsrat 2013 verabschiedet hat, wurde für alle Behörden und Einrichtungen der Verwaltungen des Bundes und der Länder ein allgemeiner Maßstab für die föderale IT-Sicherheit geschaffen. Bund und Länder haben sich darin zur gemeinsamen Abwehr von Angriffen auf Informationsinfrastrukturen in der öffentlichen Verwaltung verpflichtet. Um das gemeinsame Lagebild zu verbessern, soll der bislang freiwillige gegenseitige Austausch von Informationen zwischen Bund und Ländern über Cyber-Angriffe nunmehr verbindlich vereinbart werden.

Darüber hinaus wird der Cyber-Sicherheit auch im kommunalen Bereich zusätzliche Bedeutung beizumessen sein, zum Beispiel bei der Modernisierung des IT-Grundschutzes mit seinen organisatorischen, technischen, personellen und infrastrukturellen Empfehlungen. Der IT-Planungsrat bietet hierfür den geeigneten Rahmen. Zentrale Strukturen in den Ländern zur Beförderung von kommunaler Cyber-Sicherheit, zum Beispiel durch kommunale IT-Dienstleister, werden von der Bundesregierung unterstützt. Das Fachwissen der Bundesbehörden wird über die Länder den Kommunen künftig verstärkt zur Verfügung gestellt. Unter Einbindung der kommunalen Spitzenverbände und der Länder wird das BSI ein kommunales Lagebild erarbeiten.

Ressourcen einsetzen, Personal gewinnen und entwickeln

Cyber-Sicherheit kostet Geld. Es werden daher in den kommenden Jahren auf allen Ebenen (Bund, Länder und Kommunen) erhebliche finanzielle Anstrengungen notwendig werden, um Deutschland im Bereich Cyber-Sicherheit adäquat und nachhaltig aufzustellen.

Für die staatliche Handlungsfähigkeit kommt der Personalgewinnung und -entwicklung eine Schlüsselrolle zu. Der Leitfaden des IT-Planungsrates gibt hier wertvolle Hinweise. Es wird darum gehen, die Arbeitgeberattraktivität des Öffentlichen Dienstes offensiver darzustellen und die bestehenden dienst- und tarifrechtlichen sowie monetären Rahmenbedingungen zielgerichtet zu nutzen. Der Staat muss zudem eng mit Ausbildungseinrichtungen kooperieren. Wesentliche Erfolgsfaktoren für das Bestehen im Wettbewerb um die besten Köpfe können „Cyber-Cluster“ unter Beteiligung von Staat, Wissenschaft und Wirtschaft sein. Innerhalb der Bundesregierung ist die Personalgewinnung stärker abzustimmen. Der Personalaustausch ist zu erleichtern.

Hinzu kommt der möglichst breite Zugang zum neuen Studiengang „Cyber-Sicherheit" an der Universität der Bundeswehr in München. Fachkompetenz muss zudem auch im bestehenden Personalkörper unter Schaffung beruflicher und persönlicher Perspektiven aufgebaut und entwickelt werden, sowohl auf der Arbeits- als auch auf der Führungsebene. Der internen Aus- und Fortbildung kommt in diesem Zusammenhang eine wesentliche Bedeutung zu. An der Bundesakademie für die öffentliche Verwaltung werden entsprechende Lehrgänge zur internen Fortbildung angeboten und die Ausbildungsmodule an der Hochschule des Bundes für öffentliche Verwaltung entsprechend neu gestaltet bzw. ergänzt. Darüber hinaus bedarf es eines innovativen Personalaustauschmodells mit der Wirtschaft.

Der in der Bundeswehr betriebene Aufbau einer Cyber-Reserve kann auch für bisher Ungediente, die das bereits vorhandene Know-how von Experten aus Wirtschaft, Forschung, Verwaltung und Gesellschaft bündeln und nutzbar machen soll, als Blaupause für den Aufbau entsprechender ziviler ehrenamtlicher Strukturen dienen. Auch in diesem Zusammenhang kommt der engen Zusammenarbeit mit der deutschen IT-Sicherheitswirtschaft besondere Bedeutung zu.

Handlungsfeld 4: Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik

Ein hohes Niveau an Cyber-Sicherheit ist angesichts der transnationalen Vernetzung in einer digitalisierten Welt nur durch Einbettung und Verstärkung der nationalen Maßnahmen in die entsprechenden europäischen, regionalen und internationalen Prozessen erreichbar. Deutschland wird sich hierfür auch weiterhin aktiv in die europäische und internationale Cyber-Sicherheitspolitik einbringen. Ein klarer Rechtsrahmen, Vertrauensbildung sowie größere Resilienz in Europa und weltweit bedeuten auch mehr Schutz für Deutschland.

Sicherheit muss insbesondere im Zeitalter der Digitalisierung auch global gedacht werden. Deutschland wird sich bei Maßnahmen zur Stärkung nationaler bzw. regionaler Cyber-Sicherheitsfähigkeiten auch für interoperable Cyber-Sicherheitsarchitekturen und Standards einsetzen. Auf europäischer Ebene ist für einen sicheren europäischen Cyber-Raum der digitale Binnenmarkt mit Schwerpunkt auf dem Austausch sicherer und interoperabler Daten von entscheidender Bedeutung. Entsprechendes gilt – im Rahmen bestehender Unionskompetenzen – in Bezug auf die polizeiliche und justizielle Zusammenarbeit sowie eine entsprechend gestaltete Gemeinsame Außen- und Sicherheitspolitik und die Vernetzung der europäischen IT-Sicherheitsforschung.

Zusätzlich setzt Deutschland sich in den entsprechenden Foren für mehr Cyber-Sicherheit ein. Bei der Cyber-Verteidigungspolitik der NATO sind die Resilienz des Bündnisses und der Schutz der NATO-eigenen Netze das zentrale Ziel. Im Rahmen der Vereinten Nationen wird sich Deutschland auch weiterhin engagiert an der Klärung zahlreicher neuer Fragestellungen zur Anwendung des Völkerrechts im Cyber-Raum und seiner Weiterentwicklung und für den Erhalt und die Stärkung eines offenen, sicheren und rechtlich gestalteten Cyber-Raums einsetzen. Bilaterale Cyber-Konsultationen sowie die Zusammenarbeit mit ausgewählten Partnerländern der deutschen Entwicklungszusammenarbeit können diesen Prozess vertiefen und ein globales Minimum an Cyber-Sicherheit erreichen. Der Stärkung der internationalen Strafverfolgung kommt zudem besondere Bedeutung zu.

Bei Cyber-Angriffen unter Ausnutzung ausländischer Systeme sind regelmäßig auch die Nutzung diplomatischer Kanäle neben Maßnahmen zum Schutz und zur Wiederherstellung der beeinträchtigten Systeme und zur Verfolgung der Täter in Erwägung zu ziehen.

Strategische Ziele und Maßnahmen

Eine wirksame europäische Cyber-Sicherheitspolitik aktiv gestalten

Sicherheit ist für den gemeinsamen digitalen Binnenmarkt ein Grundpfeiler. Deutschland wird sich dafür einsetzen, dass IT-Sicherheit bei allen Digitalisierungsprozessen angemessen berücksichtigt wird, unter anderem durch eine auf Datensicherheit beruhende europäische Daten-Standortpolitik und durch Berücksichtigung von Datenschutz bei europäischen Regeln für den internationalen Datenaustausch.

EU-Pilotprojekte, bei denen die rechtlichen und technischen Fragen im Zusammenhang mit der grenzüberschreitenden Verarbeitung und Nutzung von Daten adressiert werden, sollen unter deutscher Beteiligung erfolgen. Wichtige Elemente sind die grenzüberschreitende Anwendung der elektronischen Identifizierung, der qualifizierten elektronischen Signatur, des elektronischen Siegels für Unternehmen und Behörden sowie anderer elektronischer Vertrauensdienste. Zudem wird sich Deutschland für die stärkere Berücksichtigung von Cyber-Sicherheit als Thema der Gemeinsamen Außen- und Sicherheitspolitik einsetzen. Des Weiteren wird die Bundesregierung die deutsche IT-Sicherheitsforschung darin unterstützen, sich auf europäischer Ebene zu vernetzen und in EU-Maßnahmen zu positionieren, um eine aktive Rolle bei der Gestaltung der europäischen Forschungslandschaft und der Forschungsprogramme zu übernehmen.

Die Cyber-Verteidigungspolitik der NATO weiter entwickeln

Das Nordatlantische Bündnis ist als ein Eckpfeiler der Sicherheit Deutschlands sowie der euro-atlantischen Sicherheit auf einen ausreichenden Schutz vor Angriffen aus dem Cyber-Raum angewiesen, um seine Kernaufgaben insbesondere im Bereich der kollektiven Verteidigung und bei internationalen Stabilisierungseinsätzen erfüllen zu können. Im Rahmen der Anpassung an das sich verändernde Sicherheitsumfeld muss die Allianz auch ihre Cyber-Verteidigungspolitik weiterentwickeln. Deutschland wird sich in diesen Prozess gestaltend einbringen. Ziel ist es, die Resilienz der Alliierten und der Allianz insgesamt kontinuierlich zu erhöhen und nicht zuletzt im Kontext hybrider Bedrohungen die Abschreckungs- und Verteidigungsfähigkeiten zu steigern. Die Anerkennung des Cyber-Raums als Operationsraum durch die NATO trägt der gewachsenen Bedeutung der Cyber-Verteidigungspolitik Rechnung.

Cyber-Sicherheit international aktiv mitgestalten

Innerhalb der Staatengemeinschaft sind Staaten und Regionen digital sehr unterschiedlich weit entwickelt. In den einschlägigen Foren werden zum Teil divergierende politische und wirtschaftliche Ziele verfolgt. In den Vereinten Nationen wird Deutschland weiterhin Anstöße in den Debatten zur Anwendung des Völkerrechts auf Handlungen von Staaten und nichtstaatlichen Akteuren geben: Zur Ergänzung des völkerrechtlichen Normensystems wird sich Deutschland hinsichtlich der Entwicklung von Normen, Regeln, Prinzipien sowie weiteren Empfehlungen für verantwortliches Staatenverhalten im Cyber-Raum besonders einbringen. Zudem wird Deutschland sich auch angesichts internationaler Cyber-Bedrohungen für Maßnahmen zur Wahrung internationaler Stabilität und eine Stärkung der Kapazitäten der Vereinten Nationen in diesem Bereich einsetzen. Dabei unterstützt Deutschland Überlegungen, wie auf globaler Ebene mit dem Problem der Zuordnung von Cyber-Angriffen umgegangen und der in diesem Rahmen essentielle Informationsaustausch gefördert werden kann. Wirtschaftsspionage und Cyber-Angriffe müssen durch internationale Regelungen erschwert werden, die über die deutschen und europäischen Grenzen hinweg durchsetzbar sind. Deutschland wird insbesondere internationale Bemühungen für eine Stärkung der Exportkontrollregime mit Blick auf Überwachungstechnologien aktiv unterstützen. Angesichts der Eskalationsgefahr durch Vorfälle im Cyber-Raum müssen Maßnahmen zur Vertrauensbildung umgesetzt, weiterentwickelt und ausgebaut werden. Dafür können bestehende Foren und Partnerschaften genutzt werden. Den Arbeiten in der OSZE, an denen sich Deutschland von Beginn an beteiligt hat, kommt insoweit eine Vorreiterrolle zu.

Die Bundesregierung wird zudem die Gründung eines deutschen Instituts für internationale Cyber-Sicherheit initiieren. Dessen Ziel soll es sein, Wirtschaft, Wissenschaft und staatliche Organisationen im Interesse von internationaler Stabilität und Krisenprävention einzubeziehen und Regierungen als verlässlicher und unabhängiger Kompetenzpartner beratend zur Verfügung zu stehen.

Bilaterale und regionale Unterstützung und Kooperation zum Auf- und Ausbau von Cyber-Fähigkeiten (Cyber Capacity Building)

Wo Ressourcen, Infrastruktur und Kapazitäten für Cyber-Sicherheit fehlen, entstehen besondere Bedarfe. Cyber-Bedrohungen und Angriffe können bestimmte Staaten und Bevölkerungsgruppen in ihrer wirtschaftlichen, sozialen und politischen Entwicklung stark einschränken oder zurückwerfen. Deutschland wird ausgewählte Partnerstaaten und -regionen beim Auf- und Ausbau ihrer präventiven und reaktiven Cyber-Sicherheitsfähigkeiten (Netzrobustheit und Netzresilienz) unterstützen. Dazu zählt auch die Ermutigung anderer Regionen, vertrauens- und sicherheitsbildende Maßnahmen zu vereinbaren. In ihrer Entwicklungspolitik setzt sich die Bundesregierung dafür ein, die Potenziale der Digitalisierung weltweit zu ermöglichen und damit verbundenen Risiken entgegenzuwirken. Beim Aufbau und der Unterstützung digitaler Infrastrukturen in Partnerstaaten der deutschen Entwicklungszusammenarbeit spielen auch Aspekte der Sicherheit eine besondere Rolle.

Die Bundesregierung wird weltweit als vertrauenswürdiger Akteur wahrgenommen. Auch bestehende Kompetenzen kann sie nutzen, um Partnerstaaten und -regionen zukünftig verstärkt durch Cyber Capacity Building zu unterstützen. Dies umfasst unter anderem die Entwicklung eigener Cyber-Sicherheitsstrategien, Gesetzgebungen, Institutionen, Zertifizierung, Forschung, Aus- und Weiterbildungsmaßnahmen sowie regionale Initiativen. Insbesondere dort, wo Menschen der Erstzugang zum Cyber-Raum dank entwicklungspolitischer Maßnahmen ermöglicht wird, müssen die Rahmenbedingungen und Kenntnisse für seine sichere und verlässliche Nutzung unterstützt werden.

Internationale Strafverfolgung stärken

Deutschland wird sich international für die Bekämpfung von Cyber-Kriminalität einsetzen. Die grenzüberschreitende Strafverfolgung und gemeinsame polizeiliche Ermittlungsfähigkeit werden dafür gestärkt. Die Bundesregierung wird sich für eine Verbesserung der internationalen rechtlichen Rahmenbedingungen für Gefahrenabwehr und Strafverfolgung einsetzen und sich dazu insbesondere aktiv an den auf internationaler Ebene bestehenden Initiativen zur Weiterentwicklung des Rechtsrahmens für grenzüberschreitende Ermittlungsmaßnahmen der Strafverfolgungsbehörden im Cyber-Raum beteiligen. Für eine wirksame Strafverfolgung werden zudem Möglichkeiten zur Vereinfachung und Beschleunigung von Rechtshilfeersuchen mit ausgewählten internationalen Partnern erarbeitet werden. Die Bundesregierung wird sich zudem international auch weiterhin dafür einsetzen, dass möglichst viele Staaten dem Übereinkommen des Europarates über Computerkriminalität (Budapester Konvention) beitreten und diese in nationales Recht umsetzen.

Ständiger Strategieprozess im Nationalen Cyber-Sicherheitsrat

Eine zukunftsoffene Cyber-Sicherheitsstrategie darf sich nicht allein auf die Festlegung strategischer Maßnahmen beschränken. Die Dynamik der Digitalisierung ist vielmehr durch einen ständigen Strategieprozess zu Fragen der Cyber-Sicherheit zu begleiten, aus dem sich weitere strategische Maßnahmen entwickeln können. Neue Gefahren müssen frühzeitig erkannt und innovative Lösungen erforscht und erarbeitet werden. Eine maßgebliche Rolle soll hierbei dem mit der Cyber-Sicherheitsstrategie 2011 eingerichteten Nationalen Cyber-Sicherheitsrat als strategischem Ratgeber der Bundesregierung zukommen. Der Nationale Cyber-Sicherheitsrat bringt hochrangige Vertreter von Bund (Bundesministerium des Innern, Bundeskanzleramt, Auswärtiges Amt, Bundesministerium der Verteidigung, Bundesministerium für Wirtschaft und Energie, Bundesministerium der Justiz und für Verbraucherschutz, Bundesministerium der Finanzen, Bundesministerium für Bildung und Forschung und Bundesministerium für Verkehr und digitale Infrastruktur; anlassbezogen wird der Kreis um weitere Ressorts erweitert) und Ländern sowie aus der Wirtschaft an einen Tisch und bietet somit ein geeignetes Format, um die für Deutschland im Bereich Cyber-Sicherheit wesentlichen strategischen Themen übergreifend voranzutreiben.

Im Nationalen Cyber-Sicherheitsrat werden langfristige Handlungsnotwendigkeiten und Trends identifiziert und hieraus Impulse zur Stärkung der Cyber-Sicherheit in den benannten Handlungsfeldern abgeleitet, die in die Arbeit der Bundesregierung einfließen. Bei seinen Arbeiten wird der Nationale Cyber-Sicherheitsrat in Zukunft verstärkt auch auf das Expertenwissen aus Gesellschaft, Wirtschaft und Wissenschaft zurückgreifen: Vorträge eingeladener Experten zu einzelnen strategischen Themen sollen die Diskussion und Erarbeitung von Handlungsempfehlungen vorbereiten.

In Handlungsfeld 1 soll der Nationale Cyber-Sicherheitsrat auf Basis aktueller technischer Entwicklungen insbesondere Vorschläge zur Weiterentwicklung der nationalen Regelungen für mehr Cyber-Sicherheit machen. In Handlungsfeld 2 soll er weitere Felder für die Kooperation von Staat und Wirtschaft für mehr Cyber-Sicherheit und entsprechende Umsetzungsvorschläge aufzeigen. In Handlungsfeld 3 soll sich der Nationale Cyber-Sicherheitsrat der föderalen Cyber-Sicherheitsarchitektur annehmen und wichtige Impulse in Richtung Bundesregierung und Innenministerkonferenz geben. In Handlungsfeld 4 soll der Nationale Cyber-Sicherheitsrat insbesondere den Austausch mit vergleichbaren strategischen Gremien anderer wesentlicher internationaler Partner suchen, um hieraus gegebenenfalls neue Impulse für die nationale Cyber-Sicherheitspolitik zu generieren.

Über seine zu den jeweiligen strategischen Themen erzielten Ergebnisse wird der Nationale Cyber-Sicherheitsrat das Bundeskabinett regelmäßig in Form eines schriftlichen Berichtes unterrichten. Der Bericht wird dem Kabinett zur Kenntnisnahme vorgelegt.

Glossar

Begriffsbestimmungen

Vorbemerkung: Die nachfolgenden Begriffsbestimmungen gelten für diese Cyber-Sicherheitsstrategie und sollen deren inhaltliche Klarheit und Schlüssigkeit fördern. Die Gültigkeit von in anderen Zusammenhängen im Bereich Cyber-Sicherheit gefundenen Definitionen bleibt hiervon unberührt.

Cyber-Abwehr

Cyber-Abwehr umfasst alle Maßnahmen mit dem Ziel der Wahrung oder Erhöhung der Cyber-Sicherheit.

Cyber-Angriff

Ein Cyber-Angriff ist eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyber-Raum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen.

Cyber-Raum

Der Cyber-Raum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme. Dem Cyber-Raum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, welches durch beliebige andere Datennetze erweitert werden kann.

Cyber-Sicherheit

Cyber-Sicherheit ist die IT-Sicherheit der im Cyber-Raum auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme.

Cyber-Verteidigung

Cyber-Verteidigung umfasst die in der Bundeswehr im Rahmen ihres verfassungsmäßigen Auftrages und dem völkerrechtlichen Rahmen vorhandenen defensiven und offensiven Fähigkeiten zum Wirken im Cyber-Raum, die zur Einsatz- und Operationsführung geeignet und erforderlich sind oder zur Abwehr von (militärischen) Cyber-Angriffen und damit dem Schutz eigener Informationen, IT, sowie Waffen- und Wirksysteme dienen. Dazu gehört auch die Nutzung und Mitgestaltung von Strukturen, Prozessen und Meldewesen der Cyber-Abwehr unter verteidigungsrelevanten Aspekten und Situationen.

Informationstechnik

Informationstechnik (IT) umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen.

Informationstechnisches System

Ein informationstechnisches System (IT-System) ist eine technische Anlage, die der Informationsverarbeitung dient und eine abgeschlossene Funktionseinheit bildet. Typische IT-Systeme sind Server, Clients, Einzelplatz-Computer, Mobiltelefone, Router, Switches und Sicherheitsgateways.

IT-Sicherheit

IT-Sicherheit (oder Informationssicherheit) ist die Unversehrtheit der Authentizität, Vertraulichkeit, Integrität und Verfügbarkeit eines informationstechnischen Systems und der darin verarbeiteten und gespeicherten Daten.



Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333